SUZUKI
U. S. Application No. 10/713,455
Ref. 8022-1063

This application should be rejected for the reasons given in the Reasons for Rejection Notice dated April 12, 2005. Moreover, we have reviewed the contents of the Opinion Document and Procedural Amendment, but find no grounds to reverse the reasons for rejection.

Remarks

For those keys which have a period of validity, since the sending of the period of validity along with the key when keys are sent is nothing more than which has been carried out prior to the present application as is described in Japanese Laid-Open Patent Publication H7-134547 (Paragraphs 39–50), and Japanese Laid-Open Patent Publication 2000-312711 (Paragraphs 74–77), this point cannot be considered to be anything exceptional. Therefore, the arguments in the Opinion Document cannot be accepted.

SUZUKI
U.S. Application No. 10/713,455
Our Ref. 8022-1063 (Part B)

Reason of final notice of grounds for rejection

1. This is a Notice of Grounds for Rejection which provides notification of only the rejection reason for which notification is required by the amendment included at the time of the response relative to the initial Notice of Grounds for Rejection.

Since the invention relating to the following claims of the present application could have been easily invented prior to the submission of the present application by one of ordinary skill in the technology sector to which the invention belongs based on the invention recorded in the following publications which were distributed domestically prior to the submission of the application, a patent cannot be granted, according to the stipulations of Article 29 Section 2 of the Patent Law.

Record (See the Reference Citation List to obtain the citation)

Claim 1
Citation 1

Remarks:

In Citation 1, reference is made to the fact that, in a system in which encoding processing is accomplished based on random numbers in which a transmitter accomplishes encoding processing of simple characters based on random numbers, and transmits them through a communication path, and the receiver accomplishes recovery processing of the sent encoded characters based on the same random numbers, it is provided with random numbers in which the random numbers of a specified bit length are jointly shared by the transmitter and the receiver, the transmitter accomplishing encoding processing of simple characters by means of an encoding processor which uses random numbers of a specified bit length generated from the random number sharing unit, and the receiver recovers the encoded characters by means of a recovery processor which uses random numbers of the same length as those of the transmitter. It is suggested that as the "efficacy of the invention", it is possible to apply the invention to the secret communication of real-time multimedia information, including

both image and audio information.

This being the case, constructing a scrambled broadcast system by adopting the system recorded in Citation 1 as the secret information of a real-time multimedia information which includes both image and audio would be self-evident to one skilled in the art.

Claim 2
Citations 1 and 2

Remarks:

In Citation 2, reference is made to technology for improving the reliability of preserving secrecy by encoding and recovery in which a respective encoding key and recovery key are changed to the encoding of the transmission data of a fixed number and recovery of fixed reception data based on the figures of the encoded transmission data or recovered reception data.

Also, considering the point that both Citations 1 and 2 relates to shared encoding processing technology, construction which adopts the technology recorded in Citation 2 in the system recorded in Citation 1, and changes random numbers used in encoding processing and recovery processing based on the amount of data, could be easily obtained by one skilled in the art.

Claim 3
Citation 1

Remarks:

In the notation of Citation 1, as the encoding and recovery processing, processing of a random number of a specified bit length and the exclusive theoretical sum processing of a communication message is accomplished.

Claim 4
Citations 1 and 3

Remarks:

In Citation 3, reference is made to technology which changes the column number of an encoded key corresponding to the secrecy of

the text which is the object of encoding.

Also, considering the point that Citations 1 and 3 both refer to encoding processing technology, accomplishing construction which adopts the technology recorded in a Citation 2 in the system recorded in Citation 1, and changing the number of random columns used in the encoding and recovery processing corresponding to the secrecy of the data which is the object of encoding could be easily accomplished by one skilled in the art.

Claim 5
Citation 1

Remarks:

In the notation of Citation 1, random numbers of a specified bit length generated by a random number sharing unit and encoding and recovery processing is accomplished using the two bit pattern of the block of the priority application comprising the first region of simple characters.

Claim 6
Citation 1

Remarks:

In the notation of Citation 1, reference is made to sharing random numbers of a specified bit length produced by the random number sharing unit between a transmitter and receiver. However, as other sharing technology, section [0137] discloses the transmission of a random number generated algorithm and a random number initial value as both a transmitter and the receiver are provided with a random number creation processor, and which type of random number sharing technology to adopt is something which can be appropriately determined by one skilled in the art. In addition, distributing information used in encoding processing to the reception side linked to the encoded data is disclosed in Citation 1.

Claim 7
Citation 1

Remarks:

In Citation 1, reference is made to the fact that, in a method in which encoding processing is accomplished based on random numbers in which a transmitter accomplishes encoding processing of simple characters based on random numbers, and transmits them through a communication path, and the receiver accomplishes recovery processing of the sent encoded characters based on the same random numbers, it is provided with random numbers in which the random numbers of a specified bit length are made to be jointly shared by the transmitter and the receiver, the transmitter accomplishing encoding processing of simple characters by means of an encoding processor which uses random numbers of a specified bit length generated from the random number sharing unit, and the receiver recovers the encoded characters by means of a recovery processor which uses random numbers of the same length as those of the transmitter. It is suggested that as the "efficacy of the invention", it is possible to apply to the secret communication of real-time multimedia information which includes both image and audio information.

Claim 8
Citations 1 and 2

Remarks:

In citation 2, reference is made to technology for improving the reliability of maintaining secrecy by encoding and recovery in which a respective encoding key and recovery key are changed to the encoding of transmission data of a fixed number and recovery of fixed reception data based on the figures of the encoded transmission data or recovered reception data.

Also, considering the point that both Citations 1 and 2 relate to shared encoding processing technology, construction which adopts the technology recorded in Citation 2 in the processing method recorded in Citation 1, and changes random numbers used in encoding processing and recovery processing based on the amount of data, could be easily obtained by one skilled in the art, and blocked programming with a computer at the time of accomplishing these methods is a commonly applied means to one skilled in the art.

Claim 9
Citation 1

Remarks:

In the notation of Citation 1, as the encoding and recovery processing, processing of a random number of a specified bit length and the exclusive theoretical sum processing of a communication message is accomplished.

Claim 10
Citations 1 and 3

Remarks:

In Citation 3, reference is made to technology which changes the line number of an encoded key corresponding to the secrecy of the text which is the object of encoding.

Also, considering the point that Citations 1 and 3 both record encoding processing technology, accomplishing construction which adopts the technology recorded in a Citation 2 in the processing method recorded in Citation 1, and conceiving a method which changes the number of random columns used in the encoding and recovery processing corresponding to the secrecy of the data which is the object of encoding, could be easily accomplished by one skilled in the art. The blocked programming of these methods at the time of processing by a computer is a commonly applied means to one skilled in the art.

Claim 11
Citation 1

Remarks:

In the notation of Citation 1, random numbers of a specified bit length are generated by a random number sharing unit and encoding and recovery processing is accomplished using the two bit pattern of the block of the priority application comprising the first region of simple characters.

Claim 12
Citation 1

Remarks:

In the notation of Citation 1, reference is made to sharing of random numbers of a specified bit length produced by the random number sharing unit between a transmitter and receiver. However, as other sharing technology, in section [0137] disclose both a transmitter and a receiver provided with a random number creation processor, and the transmission of a random number generated algorithm and a random number initial value, and the type of random number sharing technology to adopt is something which can be appropriately determined by one skilled in the art. In addition, distributing information used in encoding processing to the reception side linked to the encoded data is disclosed in Citation 1.

In the event that further reasons for rejection are discovered in the future, you will be notified of such reasons.

Reference Citation List

1. Japanese Laid Open Patent Publication H10-084339
2. Japanese Laid Open Patent Publication H04-072840

49200231 拒絶査定通知

整理番号:49200231　発送番号:253062　発送日:平成17年 7月 8日　1/E

拒絶査定

特許出願の番号	特願２００２－３３２４０４
起案日	平成１７年　７月　６日
特許庁審査官	中里　裕正　９３６４　５Ｓ００
発明の名称	マルチキャスト配信システムにおける鍵交換方式
特許出願人	日本電気株式会社（外　１名）
代理人	工藤　実

この出願については、平成１７年　４月１２日付け拒絶理由通知書に記載した理由によって、拒絶をすべきものである。

なお、意見書及び手続補正書の内容を検討したが、拒絶理由を覆すに足りる根拠が見いだせない。

備考

鍵に有効期限が定められているものにおいて、鍵を送信する際にその有効期限をも併せて送信することは、特開平７－１３４５４７号公報（第３９－５０段落）、特開２０００－３１２７１１号公報（第７４－７７段落）にも記載されているように本願出願前に行われていたことにすぎないから、この点を格別のものとすることはできない。

よって、意見書の所論は採用できない。

この査定に不服があるときは、この査定の謄本の送達があった日から３０日以内（在外者にあっては、９０日以内）に、特許庁長官に対して、審判を請求することができます（特許法第１２１条第１項）。

（行政事件訴訟法第４６条第２項に基づく教示）

この査定に対しては、この査定についての審判請求に対する審決に対してのみ取消訴訟を提起することができます（特許法第１７８条第６項）。

上記はファイルに記録されている事項と相違ないことを認証する。

認証日　平成17年 7月 7日　経済産業事務官　平瀬　恵美子

整理番号:49200232　発送番号:243315　発送日:平成17年 7月13日　1

拒絶理由通知書

特許出願の番号	特願２００２－３３５４０１	
起案日	平成１７年　６月２９日	
特許庁審査官	青木　重徳	４２２９　５Ｓ００
特許出願人代理人	松本　正夫　様	
適用条文	第２９条第２項	

＜＜＜＜　　最　　後　　＞＞＞＞

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

最後の拒絶理由通知とする理由

１．最初の拒絶理由通知に対する応答時の補正によって通知することが必要になった拒絶の理由のみを通知する拒絶理由通知である。

この出願の下記の請求項に係る発明は、その出願前日本国内において頒布された下記の刊行物に記載された発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　　（引用文献等については引用文献等一覧参照）

・請　求　項：１
・引用文献等：１
・備　　考

引用文献１には、送信装置が平文を乱数に基づいて暗号化処理して通信路を介して送信し、受信装置が送信された暗号文を同じ乱数に基づいて復号化処理するシステムにおいて、所定ビット長の乱数を送信装置と受信装置とで共有する乱数共有化部を備え、前記送信装置は前記乱数共有化部から生成される所定ビット長の乱数を用いて暗号化処理部により平文の暗号化を行い、前記受信装置は、前記送信装置と同じ前記所定ビット長の乱数を用いて復号化処理部により暗号文の復号化を行うことが記載されており、【発明の効果】として画像や音声を含むリアルタイム性のあるマルチメディア情報の秘密通信に適用可能であることが示唆さ

れている。

してみると、引用文献１に記載されているシステムを画像や音声を含むリアルタイム性のあるマルチメディア情報の秘密通信として採用し、スクランブル放送システムを構成できることは、当業者にとって自明なことである。

・請　求　項：２
・引用文献等：１，２
・備　　考
引用文献２には、暗号化する送信データや復号化した受信データの計数に基づいてぞれぞれ暗号鍵、復号鍵を一定数の送信データの暗号化毎ないし一定の受信データの復号毎に変更して暗号化と復号を行うことで、機密保持の信頼性を向上させる技術が記載されている。

そして、引用文献１，２が共に暗号処理技術について記載したものである点を勘案すれば、引用文献１に記載されているシステムに、引用文献２に記載されている技術を採用し、データ量に基づいて暗号化処理、復号処理に用いる乱数を変更するよう構成することは、当業者が容易になし得たことである。

・請　求　項：３
・引用文献等：１
・備　　考
引用文献１に記載されているものでは、暗号化処理や復号処理として所定ビット長の乱数と通信メッセージとの排他的論理和演算を行っている。

・請　求　項：４
・引用文献等：１，３
・備　　考
引用文献３には、暗号化の対象となる文書の機密性に応じて暗号化キーの桁数を変更する技術が記載されている。

そして、引用文献１，３が共に暗号処理技術について記載したものである点を勘案すれば、引用文献１に記載されているシステムに、引用文献２に記載されている技術を採用し、暗号化の対象となるデータの機密性に応じて暗号化処理、復号処理に用いる乱数の桁数を変更するよう構成することは、当業者が容易になし得たことである。

・請　求　項：５
・引用文献等：１
・備　　考
引用文献１に記載されているものでは、乱数共有化部によって生成された所定ビット長の乱数と、平文の第１領域である先頭ブロックの２つのビットパターン

を用いて暗号化と復号を行っている。

・請　求　項：６
・引用文献等：１
・備　　考
引用文献１に記載されているものでは、乱数共有化部により所定ビット長の乱数を送信装置と受信装置とで共有しているが、他の共有技術として例えば第【０１３７】段落において、送信装置と受信装置とが共に乱数生成処理部を備え、乱数発生アルゴリズム及び乱数初期値を伝送することが開示されていることから、どのような乱数の共有技術を採用するかは、当業者が適宜決定しうることである。また、暗号処理に用いた情報を暗号化したデータに連接して受信側に配送することは、引用文献１に開示されている。

・請　求　項：７
・引用文献等：１
・備　　考
引用文献１には、送信装置が平文を乱数に基づいて暗号化処理して通信路を介して送信し、受信装置が送信された暗号文を同じ乱数に基づいて復号化処理する処理方法において、所定ビット長の乱数を送信装置と受信装置とで共有する乱数共有化部を備え、前記送信装置は前記乱数共有化部から生成される所定ビット長の乱数を用いて暗号化処理部により平文の暗号化を行い、前記受信装置は、前記送信装置と同じ前記所定ビット長の乱数を用いて復号化処理部により暗号文の復号化を行うことが記載されており、【発明の効果】として画像や音声を含むリアルタイム性のあるマルチメディア情報の秘密通信に適用可能であることが示唆されている。
してみると、引用文献１に記載されている処理方法を画像や音声を含むリアルタイム性のあるマルチメディア情報の秘密通信として採用してスクランブル処理方法とすることは当業者にとって自明なことであるし、これら方法をコンピュータにて行う際にプログラム化することは、当業者にとって常套手段である。

・請　求　項：８
・引用文献等：１，２
・備　　考
引用文献２には、暗号化する送信データや復号化した受信データの計数に基づいてぞれぞれ暗号鍵、復号鍵を一定数の送信データの暗号化毎ないし一定の受信データの復号毎に変更して暗号化と復号を行うことで、機密保持の信頼性を向上させる技術が記載されている。
そして、引用文献１，２が共に暗号処理技術について記載したものである点を勘案すれば、引用文献１に記載されている処理方法に、引用文献２に記載されて

いる技術を採用し、データ量に基づいて暗号化処理、復号処理に用いる乱数を変更する方法を想到することは、当業者が容易になし得たことであるし、これら方法をコンピュータにて行う際にプログラム化することは、当業者にとって常套手段である。

・請　求　項：９
・引用文献等：１
・備　　考
引用文献１に記載されているものでは、暗号化処理や復号処理として所定ビット長の乱数と通信メッセージとの排他的論理和演算を行っている。

・請　求　項：１０
・引用文献等：１，３
・備　　考
引用文献３には、暗号化の対象となる文書の機密性に応じて暗号化キーの桁数を変更する技術が記載されている。
そして、引用文献１，３が共に暗号処理技術について記載したものである点を勘案すれば、引用文献１に記載されている処理方法に、引用文献２に記載されている技術を採用し、暗号化の対象となるデータの機密性に応じて暗号化処理、復号処理に用いる乱数の桁数を変更する方法を想到することは、当業者が容易になし得たことであるし、これら方法をコンピュータにて行う際にプログラム化することは、当業者にとって常套手段である。

・請　求　項：１１
・引用文献等：１
・備　　考
引用文献１に記載されているものでは、乱数共有化部によって生成された所定ビット長の乱数と、平文の第１領域である先頭ブロックの２つのビットパターンを用いて暗号化と復号を行っている。

・請　求　項：１２
・引用文献等：１
・備　　考
引用文献１に記載されているものでは、乱数共有化部により所定ビット長の乱数を送信装置と受信装置とで共有しているが、他の共有技術として例えば第【０１３７】段落において、送信装置と受信装置とが共に乱数生成処理部を備え、乱数発生アルゴリズム及び乱数初期値を伝送することが開示されていることから、どのような乱数の共有技術を採用するかは、当業者が適宜決定しうることである。また、暗号処理に用いた情報を暗号化したデータに連接して受信側に配送する

ことは、引用文献１に開示されている。

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

引　用　文　献　等　一　覧

１.特開平１０－０８４３３９号公報
２.特開平０４－０７２８４０号公報